

What is claimed is:

1. An encrypting apparatus comprising:

an encrypting operation section carrying out an encrypting operation to a plaintext using intermediate data at each of a plurality of encrypting stages of
5 said encrypting operation to produce a ciphertext, wherein said encrypting operation section outputs encrypting stage data indicating an encrypting state at each of said plurality of processing stages;

a determining section determining whether said
10 encrypting operation at a next encrypting stage should be changed, based on said encrypting stage data at a current encrypting stage from said encrypting operation section; and

a control section changing said encrypting
15 operation at said next encrypting stage when it is determined that said encrypting operation at said next encrypting stage should be changed.

2. An encrypting apparatus according to claim 1, wherein said determining section determines whether said intermediate data at said next encrypting stage of said encrypting operation should be changed
5 depending on at least a random number, based on said encrypting stage data at said current encrypting stage from said encrypting operation section,

wherein said encrypting stage data includes

000240"STES60

10 and

wherein said control section changes said intermediate data at said next encrypting stage depending on said random number.

5 place of said random number.

5 on at least a random number, based on said encrypting
stage data at said current encrypting stage from said
encrypting operation section, and

10 said encrypting operation depending on said random
number.

5. An encrypting apparatus according to claim 4, wherein said control section changes said encrypting procedure at said next encrypting stage of said

encrypting operation depending on said plaintext or a
5 data dependent on said plaintext in place of said
random number.

6. An encrypting apparatus according to claim 1,
wherein said determining section determines whether
said encrypting operation at said next encrypting
stage should be changed depending on at least a random
5 number, based on said encrypting stage data at said
current encrypting stage from said encrypting
operation section, and

wherein said control section inserts a delay
time in said encrypting operation at said next
10 encrypting stage depending on said random number.

7. An encrypting apparatus according to claim 6,
wherein said control section inserts said delay time
in said encrypting operation at said next encrypting
stage depending on said plaintext or a data dependent
5 on said plaintext in place of said random number.

8. A decrypting apparatus comprising:
a decrypting operation section carrying out a
decrypting operation to a ciphertext using
intermediate data at each of a plurality of decrypting
5 stages of said decrypting operation to produce a
plaintext, wherein said decrypting operation section

0000240"STHES60

outputs decrypting stage data indicating a decrypting state at each of said plurality of decrypting stages;

a determining section determining whether said
10 decrypting operation at a next decrypting stage should be changed, based on said decrypting stage data at a current decrypting stage from said decrypting operation section; and

a control section changing said decrypting
15 operation at said next decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed.

9. A decrypting apparatus according to claim 8, wherein said determining section determines whether said intermediate data at said next decrypting stage of said decrypting operation should be changed
5 depending on at least a random number, based on said decrypting stage data at said current decrypting stage from said decrypting operation section,

wherein said stage data includes said intermediate data for said next decrypting stage, and
10 wherein said control section changes said intermediate data at said next decrypting stage depending on said random number.

10. A decrypting apparatus according to claim 9, wherein said control section changes said intermediate

09553415 042000

data at said next decrypting stage depending on said
ciphertext or a data dependent on said ciphertext in
5 place of said random number.

11. A decrypting apparatus according to claim 8,
wherein said determining section determines whether a
decrypting procedure at said next decrypting stage of
said decrypting operation should be changed depending
5 on at least a random number, based on said stage data
at said current decrypting stage from said decrypting
operation section, and

wherein said control section changes said
decrypting procedure at said next decrypting stage of
10 said decrypting operation depending on said random
number.

12. A decrypting apparatus according to claim 11,
wherein said control section changes said decrypting
procedure at said next decrypting stage of said
decrypting operation depending on said ciphertext or a
5 data dependent on said ciphertext in place of said
random number.

13. A decrypting apparatus according to claim 8,
wherein said determining section determines whether
said decrypting operation at said next decrypting
stage should be changed depending on at least a random

00553415 042000

5 number, based on said stage data at said current
decrypting stage from said decrypting operation
section, and

wherein said control section inserts a delay
time in said decrypting operation at said next
10 decrypting stage depending on said random number.

14. A decrypting apparatus according to claim 13,
wherein said control section inserts said delay time
in said decrypting operation at said next decrypting
stage depending on said ciphertext or a data dependent
5 on said ciphertext in place of said random number.

15. An encrypting and decrypting apparatus
comprising:

an encrypting and decrypting operation section
determining whether an inputted instruction is an
5 encrypt instruction or a decrypt instruction, carrying
out an encrypting operation to an inputted text in
response to said encrypt instruction using first
intermediate data at each of a plurality of encrypting
stages of said encrypting operation to produce a
10 ciphertext, and carrying out a decrypting operation to
said inputted text in response to said decrypt
instruction using second intermediate data at each of
a plurality of decrypting stages of said decrypting
operation to produce a plaintext, wherein said

0953415 1042000

15 encrypting and decrypting operation section outputs
encrypting stage data indicating an encrypting state
at each of said plurality of encrypting stages and
outputs decrypting stage data indicating a decrypting
state at each of said plurality of decrypting stages;
20 a determining section determining whether said
encrypting operation at a next encrypting stage should
be changed, based on said encrypting stage data at a
current encrypting stage from said encrypting and
decrypting operation section, and determining whether
25 said decrypting operation at a next decrypting stage
should be changed, based on said decrypting stage data
at a current decrypting stage from said encrypting and
decrypting operation section; and
a control section changing said encrypting
30 operation at said next encrypting stage when it is
determined that said encrypting operation at said next
encrypting stage should be changed, and changing said
decrypting operation at said next decrypting stage
when it is determined that said decrypting operation
35 at said next decrypting stage should be changed.

16. An encrypting and decrypting apparatus
according to claim 15, wherein said determining
section determines whether said first intermediate
data at said next encrypting stage of said encrypting
5 operation should be changed depending on at least a

0000240" 5T4E5560

first random number, based on said encrypting stage data at said current encrypting stage from said encrypting and decrypting operation section, and determines whether said second intermediate data at
10 said next decrypting stage of said decrypting operation should be changed depending on at least a second random number, based on said decrypting stage data at said current decrypting stage from said encrypting and decrypting operation section,

15 wherein said encrypting stage data includes said first intermediate data at said next encrypting stage and said decrypting stage data includes said second intermediate data for said next decrypting stage, and

20 wherein said control section changes said first intermediate data at said next encrypting stage depending on said first random number and changes said second intermediate data at said next decrypting stage depending on said second random number.

17. An encrypting and decrypting apparatus according to claim 16, wherein said control section changes said first intermediate data at said next encrypting stage depending on said inputted text or a
5 data dependent on said inputted text in place of said first random number, and changes said second intermediate data at said next decrypting stage

0000240-572550

depending on said inputted text or said data dependent
on said inputted text in place of said second random
10 number.

18. An encrypting and decrypting apparatus
according to claim 15, wherein said determining
section determines whether an encrypting procedure at
said next encrypting stage of said encrypting
5 operation should be changed depending on at least a
first random number, based on said encrypting stage
data at said current encrypting stage from said
encrypting and decrypting operation section, and
... determines whether a decrypting procedure at said next
10 decrypting stage of said decrypting operation should
be changed depending on at least a second random
number, based on said decrypting stage data at said
current decrypting stage from said encrypting and
decrypting operation section, and

15 wherein said control section changes said
encrypting procedure at said next encrypting stage of
said encrypting operation depending on said first
random number and changes said decrypting procedure at
said next decrypting stage of said decrypting
20 operation depending on said second random number.

19. An encrypting and decrypting apparatus
according to claim 18, wherein said control section

09553415-042000

changes said encrypting procedure at said next
encrypting stage of said encrypting operation
5 depending on said inputted text or a data dependent on
said inputted text in place of said first random
number, and changes said decrypting procedure at said
next decrypting stage of said decrypting operation
depending on said inputted text or said data dependent
10 on said inputted text in place of said second random
number.

20. An encrypting and decrypting apparatus
according to claim 15, wherein said determining
section determines whether said encrypting operation
at said next encrypting stage should be changed
5 depending on at least a first random number, based on
said encrypting stage data at said current encrypting
stage from said encrypting and decrypting operation
section, and determines whether said decrypting
operation at said next decrypting stage should be
10 changed depending on at least a second random number,
based on said decrypting stage data at said current
decrypting stage from said encrypting and decrypting
operation section, and

wherein said control section inserts a first
15 delay time in said encrypting operation at said next
encrypting stage depending on said first random number
and inserts a second delay time in said decrypting

09553415"042000

operation at said next decrypting stage depending on said second random number.

21. An encrypting and decrypting apparatus according to claim 20, wherein said control section inserts said first delay time in said encrypting operation at said next encrypting stage depending on
5 said inputted text or a data dependent on said inputted text in place of said first random number, and inserts said second delay time in said decrypting operation at said next decrypting stage depending on said inputted text or said data dependent on said
10 inputted text in place of said second random number.

22. An encrypting method comprising:

(a) determining whether an encrypting operation at a current encrypting stage should be changed, based on encrypting stage data at a previous encrypting
5 stage, said encrypting stage data at said previous encrypting stage indicating an encrypting state at said previous encrypting stage;

(b) changing said encrypting operation at said current encrypting stage when it is determined that
10 said encrypting operation at said current encrypting stage should be changed;

(c) carrying out said encrypting operation at said current encrypting stage to a plaintext using

000240" 5742550

intermediate data at said current encrypting stage;

15 and

(d) executing said steps (a) to (c) to each of
a plurality of said encrypting stages of said
encrypting operation to produce a ciphertext.

23. An encrypting method according to claim 22,
wherein said determining includes:

determining whether said intermediate data at
said current encrypting stage of said encrypting
5 operation should be changed depending on at least a
random number, based on said encrypting stage data at
said previous encrypting stage,

wherein said encrypting stage data includes
said intermediate data at said current encrypting
10 stage, and

wherein said changing includes:

changing said intermediate data at said current
encrypting stage depending on said random number.

24. An encrypting method according to claim 23,
wherein said changing includes:

changing said intermediate data at said current
encrypting stage depending on said plaintext or a data
5 dependent on said plaintext in place of said random
number.

000240" 5TH E5560

determining whether an encrypting procedure at said current encrypting stage of said encrypting operation should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage, and

changing said encrypting procedure at said
10 current encrypting stage of said encrypting operation
depending on said random number.

changing said encrypting procedure at said next encrypting stage of said encrypting operation depending on said plaintext or a data dependent on said plaintext in place of said random number.

determining whether said encrypting operation at said current encrypting stage should be changed depending on at least a random number, based on said encrypting stage data at said previous encrypting stage, and

wherein said changing includes:

inserting a delay time in said encrypting
10 operation at said current encrypting stage depending
on said random number.

28. An encrypting method according to claim 27,
wherein said changing includes:

inserting said delay time in said encrypting
operation at said current encrypting stage depending
5 on said plaintext or a data dependent on said
plaintext in place of said random number.

29. A decrypting method comprising:

(a) determining whether a decrypting operation
at a current decrypting stage should be changed, based
on decrypting stage data at a previous decrypting
5 stage, said decrypting stage data at said previous
decrypting stage indicating an decrypting state at
each of said plurality of processing stages;

(b) changing said decrypting operation at said
current decrypting stage when it is determined that
10 said decrypting operation at said next decrypting
stage should be changed;

(c) carrying out said decrypting operation at
said current decrypting stage to a ciphertext using
intermediate data at said current decrypting stage;
15 and

(d) executing said steps (a) to (c) to each of

09553415 "042000

a plurality of decrypting stages to produce a plaintext.

30. A decrypting method according to claim 29, wherein said determining includes:

determining whether said intermediate data at said current decrypting stage of said decrypting operation should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage,

wherein said stage data includes said intermediate data at said current decrypting stage, and

wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said random number.

31. A decrypting method according to claim 30, wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said ciphertext or a data dependent on said ciphertext in place of said random number.

32. A decrypting method according to claim 29, wherein said determining includes:

determining whether a decrypting procedure at

000240" STES560

5 operation should be changed depending on at least a
random number, based on said decrypting stage data at
said previous decrypting stage, and

wherein said changing includes:

changing said decrypting procedure at said
10 current decrypting stage of said decrypting operation
depending on said random number.

33. A decrypting method according to claim 32,
wherein said changing includes:

changing said decrypting procedure at said
current decrypting stage of said decrypting operation
5 depending on said ciphertext or a data dependent on
said ciphertext in place of said random number.

34. A decrypting method according to claim 29,
wherein said determining includes:

determining whether said decrypting operation at said current decrypting stage should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage, and

wherein said changing includes:

```

            inserting a delay time in said decrypting
10 operation at said current decrypting stage depending
            on said random number.

```


35. A decrypting method according to claim 34,
wherein said changing includes:

inserting said delay time in said decrypting
operation at said current decrypting stage depending
5 on said ciphertext or a data dependent on said
ciphertext in place of said random number.

36. An encrypting and decrypting method comprising:

(a) determining whether an inputted instruction
is an encrypt instruction or a decrypt instruction;

(b) determining whether said encrypting
5 operation to a text at a current encrypting stage of
an encrypting operation should be changed, based on
said encrypting stage data at a previous encrypting
stage, said encrypting stage data at said current
encrypting stage indicating an encrypting state at
10 said current encrypting stage;

(c) changing said encrypting operation to said
text at said current encrypting stage when it is
determined that said encrypting operation to said text
at said current encrypting stage should be changed;

15 (d) carrying out said encrypting operation to
said text using first intermediate data at current
encrypting stage of said encrypting operation;

(e) executing said steps (b) to (d) for each of
a plurality of encrypting stages of said encrypting
20 operation to said text in response to said encrypt

09553415-042000

instruction to produce a ciphertext;

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data
25 at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage;

(g) changing said decrypting operation to said text at said current decrypting stage when it is
30 determined that said decrypting operation to said text at said current decrypting stage should be changed;

(h) carrying out said decrypting operation to said text using second intermediate data at said current decrypting stage; and

35 (i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting operation to said text in response to said decrypt instruction to produce a plaintext.

37. An encrypting and decrypting method according to claim 36, wherein said (b) determining includes:

determining whether said first intermediate data at said current encrypting stage of said
5 encrypting operation should be changed depending on at least a first random number, based on said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

09553415-042000

determining whether said second intermediate
10 data at said current decrypting stage of said
decrypting operation should be changed depending on at
least a second random number, based on said decrypting
stage data at said previous decrypting stage,

wherein said encrypting stage data includes
15 said first intermediate data at said current
encrypting stage and said decrypting stage data
includes said second intermediate data for said
current decrypting stage,

wherein said (c) changing includes:

changing said first intermediate data at said current encrypting stage depending on said first random number, and

wherein said (g) changing includes:

25 current decrypting stage depending on said second
random number.

38. An encrypting and decrypting method according to claim 37, wherein said (c) changing includes:

changing said first intermediate data at said
current encrypting stage depending on said text or a
5 data dependent on said text in place of said first
random number, and

wherein said (g) changing includes:

current decrypting stage depending on said text or
10 said data dependent on said text in place of said
second random number.

39. An encrypting and decrypting method according
to claim 36, wherein said (b) determining includes:

determining whether an encrypting procedure at
said current encrypting stage of said encrypting
5 operation should be changed depending on at least a
first random number, based on said encrypting stage
data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether a decrypting procedure at
10 said current decrypting stage of said decrypting
operation should be changed depending on at least a
second random number, based on said decrypting stage
data at said previous decrypting stage,

wherein said (c) changing includes:

15 changing said encrypting procedure at said
current encrypting stage of said encrypting operation
depending on said first random number, and

wherein said (g) changing includes:

changing said decrypting procedure at said
20 current decrypting stage of said decrypting operation
depending on said second random number.

40. An encrypting and decrypting method according

0000240"STES560

to claim 39, wherein said (c) changing includes:

changing said encrypting procedure at said
current encrypting stage of said encrypting operation
5 depending on said text or a data dependent on said
text in place of said first random number, and

wherein said (g) changing includes:

changing said decrypting procedure at said
current decrypting stage of said decrypting operation
10 depending on said text or said data dependent on said
text in place of said second random number.

41. An encrypting and decrypting method according
to claim 36, wherein said (b) determining includes:

determining whether said encrypting operation
at said current encrypting stage should be changed
5 depending on at least a first random number, based on
said encrypting stage data at said previous encrypting
stage,

wherein said (f) determining includes:

determining whether said decrypting operation
10 at said current decrypting stage should be changed
depending on at least a second random number, based on
said decrypting stage data at said previous decrypting
stage,

wherein said (c) changing includes:

15 inserting a first delay time in said encrypting
operation at said current encrypting stage depending

000240" STHESS60

on said first random number, and

wherein said (g) changing includes:

inserting a second delay time in said

20 decrypting operation at said current decrypting stage
depending on said second random number.

42. An encrypting and decrypting method according
to claim 41, wherein said (c) changing includes:

inserting said first delay time in said
encrypting operation at said current encrypting stage
5 depending on said text or a data dependent on said
text in place of said first random number,

wherein said (f) changing includes:

inserting said second delay time in said
decrypting operation at said current decrypting stage
10 depending on said text or said data dependent on said
text in place of said second random number.

43. A recording medium which stores a problem for
an encrypting method, wherein said encrypting method
comprises:

(a) determining whether an encrypting operation
5 at a current encrypting stage should be changed, based
on encrypting stage data at a previous encrypting
stage, said encrypting stage data at said previous
encrypting stage indicating an encrypting state at
said previous encrypting stage;

000020"STES60
09553415-042000

10 (b) changing said encrypting operation at said
current encrypting stage when it is determined that
said encrypting operation at said current encrypting
stage should be changed;

(c) carrying out said encrypting operation at
15 said current encrypting stage to a plaintext using
intermediate data at said current encrypting stage;
and

(d) executing said steps (a) to (c) to each of
a plurality of said encrypting stages of said
20 encrypting operation to produce a ciphertext.

44. A recording medium according to claim 43,
wherein said determining includes:

determining whether said intermediate data at
said current encrypting stage of said encrypting
5 operation should be changed depending on at least a
random number, based on said encrypting stage data at
said previous encrypting stage,

wherein said encrypting stage data includes
said intermediate data at said current encrypting
10 stage, and

wherein said changing includes:

changing said intermediate data at said current
encrypting stage depending on said random number.

45. A recording medium according to claim 44,

0000240"STE5560

wherein said changing includes:

changing said intermediate data at said current
encrypting stage depending on said plaintext or a data
5 dependent on said plaintext in place of said random
number.

46. A recording medium according to claim 43,
wherein said determining includes:

determining whether an encrypting procedure at
said current encrypting stage of said encrypting
5 operation should be changed depending on at least a
random number, based on said encrypting stage data at
said previous encrypting stage, and

wherein said changing includes:

changing said encrypting procedure at said
10 current encrypting stage of said encrypting operation
depending on said random number.

47. A recording medium according to claim 46,
wherein said changing includes:

changes said encrypting procedure at said next
encrypting stage of said encrypting operation
5 depending on said plaintext or a data dependent on
said plaintext in place of said random number.

48. A recording medium according to claim 43,
wherein said determining includes:

000240"STES60

determining whether said encrypting operation
at said current encrypting stage should be changed
5 depending on at least a random number, based on said
encrypting stage data at said previous encrypting
stage, and

wherein said changing includes:

inserting a delay time in said encrypting
10 operation at said current encrypting stage depending
on said random number.

49. A recording medium according to claim 48,
wherein said changing includes:

inserting said delay time in said encrypting
operation at said current encrypting stage depending
5 on said plaintext or a data dependent on said
plaintext in place of said random number.

50. A recording medium which stores a program for a
decrypting method, wherein said decrypting method
comprises:

(a) determining whether a decrypting operation
5 at a current decrypting stage should be changed, based
on decrypting stage data at a previous decrypting
stage, said decrypting stage data at said previous
decrypting stage indicating an decrypting state at
each of said plurality of processing stages;

10 (b) changing said decrypting operation at said

0000240" 5TH E550

current decrypting stage when it is determined that said decrypting operation at said next decrypting stage should be changed;

(c) carrying out said decrypting operation at
15 said current decrypting stage to a ciphertext using intermediate data at said current decrypting stage; and

(d) executing said steps (a) to (c) to each of a plurality of decrypting stages to produce a
20 plaintext.

51. A recording medium according to claim 50, wherein said determining includes:

determining whether said intermediate data at said current decrypting stage of said decrypting
5 operation should be changed depending on at least a random number, based on said decrypting stage data at said previous decrypting stage,

wherein said stage data includes said intermediate data at said current decrypting stage,
10 and

wherein said changing includes:

changing said intermediate data at said current decrypting stage depending on said random number.

52. A recording medium according to claim 51, wherein said changing includes:

09553415.042000

changing said intermediate data at said current
decrypting stage depending on said ciphertext or a
5 data dependent on said ciphertext in place of said
random number.

53. A recording medium according to claim 50,
wherein said determining includes:

determining whether a decrypting procedure at
said current decrypting stage of said decrypting
5 operation should be changed depending on at least a
random number, based on said decrypting stage data at
said previous decrypting stage, and

wherein said changing includes:

changing said decrypting procedure at said
10 current decrypting stage of said decrypting operation
depending on said random number.

54. A recording medium according to claim 53,
wherein said changing includes:

changing said decrypting procedure at said
current decrypting stage of said decrypting operation
5 depending on said ciphertext or a data dependent on
said ciphertext in place of said random number.

55. A recording medium according to claim 50,
wherein said determining includes:

determining whether said decrypting operation

09553415 1042000

at said current decrypting stage should be changed
5 depending on at least a random number, based on said
decrypting stage data at said previous decrypting
stage, and

wherein said changing includes:

inserting a delay time in said decrypting
10 operation at said current decrypting stage depending
on said random number.

56. A recording medium according to claim 55,
wherein said changing includes:

inserting said delay time in said decrypting
operation at said current decrypting stage depending
5 on said ciphertext or a data dependent on said
ciphertext in place of said random number.

57. A recording medium which stores a problem for
an encrypting and decrypting method, wherein said
encrypting and decrypting method comprises:

(a) determining whether an inputted instruction
5 is an encrypt instruction or a decrypt instruction;

(b) determining whether said encrypting
operation to a text at a current encrypting stage of
an encrypting operation should be changed, based on
said encrypting stage data at a previous encrypting
10 stage, said encrypting stage data at said current
encrypting stage indicating an encrypting state at

09553415-042000

```

said current encrypting stage;

```

(d) carrying out said encrypting operation to said text using first intermediate data at current encrypting stage of said encrypting operation;

(f) determining whether said decrypting operation to said text at a current decrypting stage should be changed, based on said decrypting stage data at a previous decrypting stage, said decrypting stage data at said current decrypting stage indicating an decrypting state at said current decrypting stage;

30 (g) changing said decrypting operation to said text at said current decrypting stage when it is determined that said decrypting operation to said text at said current decrypting stage should be changed;

(h) carrying out said decrypting operation to
35 said text using second intermediate data at said
current decrypting stage; and

(i) executing said steps (f) to (h) for each of a plurality of decrypting stages of said encrypting

operation to said text in response to said decrypt
40 instruction to produce a plaintext.

58. A recording medium according to claim 57,
wherein said (b) determining includes:

determining whether said first intermediate
data at said current encrypting stage of said
5 encrypting operation should be changed depending on at
least a first random number, based on said encrypting
stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said second intermediate
10 data at said current decrypting stage of said
decrypting operation should be changed depending on at
least a second random number, based on said decrypting
stage data at said previous decrypting stage,

wherein said encrypting stage data includes
15 said first intermediate data at said current
encrypting stage and said decrypting stage data
includes said second intermediate data for said
current decrypting stage,

wherein said (c) changing includes:

20 changing said first intermediate data at said
current encrypting stage depending on said first
random number, and

wherein said (g) changing includes:

changing said second intermediate data at said

09553415.042000

25 current decrypting stage depending on said second
random number.

59. A recording medium according to claim 58,
wherein said (c) changing includes:

changing said first intermediate data at said
current encrypting stage depending on said text or a
5 data dependent on said text in place of said first
random number, and

wherein said (g) changing includes:

changing said second intermediate data at said
current decrypting stage depending on said text or
10 said data dependent on said text in place of said
second random number.

60. A recording medium according to claim 57,
wherein said (b) determining includes:

determining whether an encrypting procedure at
said current encrypting stage of said encrypting
5 operation should be changed depending on at least a
first random number, based on said encrypting stage
data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether a decrypting procedure at
10 said current decrypting stage of said decrypting
operation should be changed depending on at least a
second random number, based on said decrypting stage

000240" STE5560

data at said previous decrypting stage,

wherein said (c) changing includes:

15 changing said encrypting procedure at said
current encrypting stage of said encrypting operation
depending on said first random number, and

wherein said (g) changing includes:

changing said decrypting procedure at said
20 current decrypting stage of said decrypting operation
depending on said second random number.

61. A recording medium according to claim 60,
wherein said (c) changing includes:

changing said encrypting procedure at said
current encrypting stage of said encrypting operation
5 depending on said text or a data dependent on said
text in place of said first random number, and

wherein said (g) changing includes:

changing said decrypting procedure at said
current decrypting stage of said decrypting operation
10 depending on said text or said data dependent on said
text in place of said second random number.

62. A recording medium according to claim 57,
wherein said (b) determining includes:

determining whether said encrypting operation
at said current encrypting stage should be changed
5 depending on at least a first random number, based on

0000240"STES60

said encrypting stage data at said previous encrypting stage,

wherein said (f) determining includes:

determining whether said decrypting operation
10 at said current decrypting stage should be changed
depending on at least a second random number, based on
said decrypting stage data at said previous decrypting
stage,

wherein said (c) changing includes:

15 inserting a first delay time in said encrypting
operation at said current encrypting stage depending
on said first random number, and

wherein said (g) changing includes:

inserting a second delay time in said
20 decrypting operation at said current decrypting stage
depending on said second random number.

63. A recording medium according to claim 62,
wherein said (c) changing includes:

inserting said first delay time in said
encrypting operation at said current encrypting stage
5 depending on said text or a data dependent on said
text in place of said first random number,

wherein said (f) changing includes:

inserting said second delay time in said
decrypting operation at said current decrypting stage
10 depending on said text or said data dependent on said

09553415 042000

text in place of said second random number.

09553415 042000